第一章

再探群、环、域

从本册开始, 我们将学习抽象代数部分. 抽象代数也称为近世代数, 它通常被认为是以 Galois (伽罗瓦) 理论的产生作为分界线的, 而在此之前的古典代数学则着重于研究求解代数方程. 法国数学家 Galois 在 19 世纪二三十年代用群的观点来研究代数方程的解, 证明了一般的高于四次的代数方程没有根式解. Galois 理论再加上其他一些学科的需要, 代数学的研究逐渐转为研究各种代数结构和它们的运算性质. 特别是 20 世纪以来, 数学得到了蓬勃发展, 很多数学分支中都出现了代数结构, 这样代数学自然就渗透到这些数学分支中, 成为它们的基础.

为什么要研究代数结构的运算性质? 实际上求解代数问题利用的就是代数结构的运算性质.

例 1.0.1　解一元一次方程 $ax = b$, 其中 a, b 为已知数 (有理数或实数或复数或某个数域中的数), x 为未知数.

若 $a \neq 0$, 方程两端同时乘 a^{-1} 得到 $x = a^{-1}b$, 这里用到

$$a^{-1}(ax) = (a^{-1}a)x = 1 \cdot x = x.$$

(这需要存在数 1, 非零数 a 有逆 (倒数), 乘法满足结合律.)

若 $a = 0$, 则不论 x 取何值, 方程左端总为 0 (这需要 0 乘任何数均为 0). 所以若 $b \neq 0$, 则方程无解; 若 $b = 0$, 则 x 取任何数都是方程的解.

注意到我们在解决代数问题时用到的运算性质必须是所给的代数结构中具有的. 如在域中确实存在例 1.0.1 中需要的运算性质, 但在其他代数结构中却并不总是这样. 如在整数环中解方程 $3x = 6$, 虽然我们知道它的解为 $x = 2$, 但这却不能通过在方程两端同时乘系数 3 的逆得到. 因为在整数环中, 3 的逆是不存在的, 而不存在的事物是不能被使用的.

这是一个典型的代数问题, 特点是对一类问题 (不只是单个问题) 利用统一的方法 (即运算性质) 求出所有可能的解答, 故运算性质是解决代数问题的关键所在. 在解决各种问题的过程中, 人们常常主动地把与此问题有关的对象 (某个有特定关系的集合) 组织成一个可运算的结构并研究它的运算性质, 这个带有运算的集合就是代数结构. 下面我们看一个为解决问题而引入的代数结构的例子.

例 1.0.2　为解决 $x^2 + 1 = 0$ 在实数域 $\mathbb{R}$ 中无解的问题, 取 $\mathbb{R}$ 上的 2 维向量集

$$\mathbb{R}^2 = \{(a, b) \mid a, b \in \mathbb{R}\},$$

在其上定义加法和乘法为

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b)(c, d) = (ac - bd, ad + bc).$$

则 $\mathbb{R}^2$ 有着和 $\mathbb{R}$ 相同的运算性质 (加法和乘法的交换律和结合律, 乘法关于加法的分配律, 每个数有负数, 非零数有倒数等), 并且 $x^2 + 1 = 0$ 在其中有解 $(0, \pm 1)$. 注意到在 $\mathbb{R}^2$

中, 每个实数 a 被写成 $(a,0)$, 即 $1=(1,0)$, $0=(0,0)$. 实际上这个 $\mathbb{R}^2$ 在如上加法和乘法下就是复数域.

随着代数学的发展, 人们引入了许多带有运算的结构, 开始是单个地、独立地研究各个具体的带有运算的结构. 但人们逐渐发现, 许多带有运算的结构有相同的运算性质, 可以抽象出来进行讨论, 抽象讨论得到的结果适用于具体的带有运算的结构. 英国著名哲学家 Alfred North Whitehead (怀特海) 说: "最高的抽象是控制我们对具体事物的思想的真正武器." 抽象是代数学研究乃至整个数学研究中最常用的手段. 直观地说, 给定一个抽象的非空集合, 在其中定义一些运算, 满足一些运算法则 (称为公理). 一组公理就定义了一种代数结构, 代数学就是在这些公理的基础上来研究代数结构的运算性质.

《代数学 (一)》中已经定义了群、环、域、模等代数结构, 给出了一些群、环、域的例子, 并详细地讨论了线性空间这种代数结构. 在接下来的抽象代数部分, 我们将进一步讨论群、环、域、模等代数结构和它们的运算性质. 作为开篇, 本章再次给出群、环、域这三种代数结构的定义、基本性质和更多的例子. 为了叙述清楚, 下面用符号 $\mathbb{Z}$ 表示整数集, $\mathbb{Z}^+$ 表示正整数集, $\mathbb{N}=\mathbb{Z}^+\cup\{0\}$ 表示自然数 (非负整数) 集, $\mathbb{Q}$ 表示有理数集, $\mathbb{R}$ 表示实数集, $\mathbb{C}$ 表示复数集.

1.1 运算与运算法则

代数结构的灵魂就是运算, 代数结构的运算性质就是其中的运算所满足的结论. 小学时我们就熟悉了整数及分数的四则运算, 《代数学 (一)》中给出了运算的严格定义, 本书的前两册中我们学习了矩阵的加法和乘法运算、向量的加法运算、实向量的内积运算等. 下面再复述一下运算这个概念.

设 A, B, C 是三个非空集合, 一个 $A\times B$ 到 C 的映射称为 A 与 B 到 C 的**代数运算**. 特别地, 当 $A=B=C$ 时, 这样的代数运算也称为 A 上的一个**代数运算** (或称为 A 上的一个**二元运算**, 也简称为**运算**). 换句话说, 集合 A 上的代数运算是一个对应法则, 使得对于 A 中任意两个元素 a, b (它们可以相同), 按这个法则都有 A 中唯一一个元素 c 与其对应, 而 c 也称为元素 a, b 在此代数运算下的运算结果. 所以运算的核心是运算结果唯一并且运算结果还在集合 A 中.

例 1.1.1 设 $F^{m\times n}$ 是域 F 上的所有 $m\times n$ 矩阵构成的集合, 显然矩阵加法是 $F^{m\times n}$ 上的一个运算, 但若 $m\neq n$, 两个 $m\times n$ 矩阵不能相乘, 所以通常的矩阵乘法不是 $F^{m\times n}$ 上的运算. 若 $m=n$, 显然通常的矩阵乘法是 $F^{n\times n}$ 上的运算.

仍然考虑集合 $F^{m\times n}$, 任取 $P=(p_{ij})_{m\times n}$, $Q=(q_{ij})_{m\times n}\in F^{m\times n}$, 定义

$$P \circ Q = (p_{ij}q_{ij})_{m\times n},$$

则 $\circ$ 是 $F^{m\times n}$ 上的运算, 称其为矩阵的 **Hadamard (阿达马) 乘积**.

下面总假设非空集合 A 上有一个运算, 为方便起见, 把 A 上的这个运算称为乘法, 记为 "$\cdot$". A 中元素 a 和 b 的运算结果记为 $a\cdot b$, 或简记为 ab, 也称其为 a 与 b 的**积**. 对于 $a,b\in A$, 若 $a=b$, 则对任意 $c\in A$ 有 $(a,c)=(b,c)\in A^2$, 由运算结果的唯一性有 $ac=bc$. 类似地有 $ca=cb$, 分别称为等式 $a=b$ 两端同时右乘 c 或同时左乘 c.

对于 $a,b\in A$, ab 是 A^2 中元素 (a,b) 在该运算下的像, 而 ba 是 A^2 中元素 (b,a) 在该运算下的像. 若 $a\neq b$, 则 $(a,b)\neq(b,a)$, 所以对运算结果来说, 我们不能指望一定有 $ab=ba$. 但特别地, 若 $ab=ba$, 则称 a, b 在该运算下**可交换**. 若对任意的 a, $b\in A$, a 和 b 在运算下均可交换, 即均有 $ab=ba$, 则称该运算满足**交换律**. 例如通常数的加法和乘法运算、矩阵的加法运算、向量的加法运算都满足交换律, 例 1.1.1 中矩阵的 Hadamard 乘积运算也满足交换律. 但当 $n\geqslant 2$ 时, $F^{n\times n}$ 上通常的矩阵乘法运算则不满足交换律. 一般说来, 映射的合成运算也不满足交换律.

前面定义的集合 A 上的运算是二元运算, 即在该运算下集合 A 中的两个元素 a 和 b 有唯一的一个运算结果 ab. 那么对于 A 中的多个元素又当如何? 它们可以运算吗? 对集合 A 中的多个元素, 为了运算, 这需要组合成多次二元运算, 而组合是通过加括号来完成的, 但是元素的前后次序不能改变. 例如对于三个元素 a, b, $c\in A$, 可以通过加括号组合成两种运算方式, 即 $(ab)c$ 和 $a(bc)$, 前一种方式是先计算 ab, 再计算 A 中的元素 ab 和 c 的乘积. 后一种方式是先计算 bc, 再计算 A 中的元素 a 和 bc 的乘积. 对于 A 中四个元素 a, b, c, d, 有如下 5 种不同的运算方式, 分别为 $((ab)c)d$, $(a(bc))d$, $(ab)(cd)$, $a((bc)d)$, $a(b(cd))$.

如果对 A 中任意三个元素 a, b, $c\in A$, 均有

$$(ab)c=a(bc),$$

即它们组合成二元运算的两种运算方式的运算结果相等, 就称 A 上的该运算满足**结合律**. 例如通常数的加法和乘法运算、矩阵的加法和乘法运算、向量的加法运算、映射的合成运算都满足结合律, 例 1.1.1 中矩阵的 Hadamard 乘积运算也满足结合律. 而通常数的减法运算不满足结合律.

定理 1.1.1　*若集合 A 上的运算有结合律, 则有广义结合律, 即对 A 中任意 $n\geqslant 3$ 个元素 $a_1, a_2, \cdots, a_n$ 组合成的多种运算方式所得的运算结果都相等.*

证明　记

$$a_1a_2\cdots a_n=(\cdots(((a_1a_2)a_3)a_4)\cdots a_{n-1})a_n,$$

即按照从前往后的方式组合所得的运算结果. 设 $\varphi(a_1,a_2,\cdots,a_n)$ 是任意一种组合成的

运算方式的运算结果, 广义结合律即为

$$\varphi(a_1, a_2, \cdots, a_n) = a_1 a_2 \cdots a_n.$$

下面通过对 n 做归纳来证明. $n = 3$ 时即为结合律, 结论显然成立. 设 $n > 3$ 且结论对任意 $m < n$ 已经成立.

对任一 $\varphi(a_1, a_2, \cdots, a_n)$, 这个乘积的最后一次乘法一定是对某个 $m < n$, 由 a_1, $a_2, \cdots, a_m$ 的某个乘积 $\varphi_1(a_1, a_2, \cdots, a_m)$ 和 $a_{m+1}, a_{m+2}, \cdots, a_n$ 的某个乘积 $\varphi_2(a_{m+1}, a_{m+2}, \cdots, a_n)$ 做乘积, 即

$$\varphi(a_1, a_2, \cdots, a_n) = \varphi_1(a_1, a_2, \cdots, a_m)\varphi_2(a_{m+1}, a_{m+2}, \cdots, a_n).$$

由归纳假设, $\varphi_1(a_1, a_2, \cdots, a_m) = a_1 a_2 \cdots a_m$, $\varphi_2(a_{m+1}, a_{m+2}, \cdots, a_n) = a_{m+1} a_{m+2} \cdots a_n$. 如果 $m + 1 = n$, 那么

$$\varphi_1(a_1, a_2, \cdots, a_m)\varphi_2(a_{m+1}, a_{m+2}, \cdots, a_n) = (a_1 a_2 \cdots a_m)a_n = a_1 a_2 \cdots a_n.$$

如果 $m + 1 < n$, 由运算满足结合律, 有

$$\begin{aligned}
\varphi_1(a_1, a_2, \cdots, a_m)\varphi_2(a_{m+1}, a_{m+2}, \cdots, a_n) &= (a_1 a_2 \cdots a_m)(a_{m+1} a_{m+2} \cdots a_n) \\
&= (a_1 a_2 \cdots a_m)((a_{m+1} a_{m+2} \cdots a_{n-1})a_n) \\
&= ((a_1 a_2 \cdots a_m)(a_{m+1} a_{m+2} \cdots a_{n-1}))a_n \\
&= (a_1 a_2 \cdots a_{n-1})a_n \\
&= a_1 a_2 \cdots a_n.
\end{aligned}$$

从而结论对 n 成立. 由归纳法原理, 定理对任意正整数 $n \geqslant 3$ 成立. □

上面定理表明, 若 A 上的运算有结合律, 则 A 中任意有限个元素组合成的多种运算方式的运算结果都相等, 这可以让我们自由地讨论多个元素组合的运算. 为此下面我们讨论的代数结构中的运算都满足结合律, 并用 $a_1 a_2 \cdots a_n$ 来表示 n 个元素 a_1, a_2, $\cdots$, a_n 的任一种组合方式所得到的运算结果. 特别地, 设 n 为正整数, 若 $a_1 = a_2 = \cdots = a_n = a$, 则记

$$a^n = \underbrace{a a \cdots a}_{n\text{ 个}},$$

并称 a^n 为 a 的 n **次幂** (或 n **次方**). 显然, 对任意正整数 m, n, 有

$$a^m a^n = a^{m+n}$$

和

$$(a^m)^n = a^{mn}.$$

定义 1.1.1　*A 中元素 e 称为*单位元*, 若对任意 $a \in A$ 均有 $ea = ae = a$.*

命题 1.1.1　*设 A 有单位元, 则单位元是唯一的.*

证明　设 e_1 和 e_2 都是 A 的单位元, 则由单位元的定义有

$$e_2 = e_1 e_2 = e_1.$$

□

若 A 有单位元 e, 对任意 $a \in A$, 定义 $a^0 = e$, 即在有单位元的代数结构中定义每个元素的 0 次幂均为单位元.

定义 1.1.2　*设 A 有单位元 e, $a \in A$, 若存在 $b \in A$ 使得*

$$ab = ba = e,$$

则称元素 a 可逆, 而元素 b 称为元素 a 的一个逆元.

由定义可以看出, 讨论 A 中元素是否可逆是在 A 有单位元的前提下进行的. 所以后面说到元素可逆时, 该代数结构必须有单位元, 而为简洁起见, 这一点我们以后就不重复说了.

命题 1.1.2　*设 A 上的运算满足结合律, 若 $a \in A$ 可逆, 则 a 的逆元唯一.*

证明　设 b_1 和 b_2 都是 a 的逆元, e 为 A 的单位元, 则有

$$b_2 = eb_2 = (b_1 a)b_2 = b_1(ab_2) = b_1 e = b_1.$$

□

由该命题, 运算具有结合律的代数结构中的可逆元的逆元唯一, 下面就用 a^{-1} 来记可逆元 a 的唯一逆元.

命题 1.1.3　*设 A 上的运算满足结合律, 若 $a \in A$ 可逆, 则 a^{-1} 也可逆, 且 $(a^{-1})^{-1} = a$. 进一步地, 若两个元素 a, b 都可逆, 则它们的乘积 ab 也可逆, 且*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

证明　仍用 e 表示 A 中的单位元, 由定义有

$$aa^{-1} = a^{-1}a = e,$$

由此立得 a^{-1} 可逆, 且 $(a^{-1})^{-1} = a$.

设 $a, b \in A$ 都可逆, 则由广义结合律有

$$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e.$$

同样地, 可以证明 $(b^{-1}a^{-1})(ab) = e$, 所以 ab 可逆且

$$(ab)^{-1} = b^{-1}a^{-1}.$$

□

类似地, 若 A 上的运算满足结合律, 归纳可证若 $a_1, a_2, \cdots, a_m \in A$ 均可逆, 则 $a_1a_2\cdots a_m$ 也可逆, 且其逆元

$$(a_1a_2\cdots a_m)^{-1} = a_m^{-1}\cdots a_2^{-1}a_1^{-1}.$$

该结论通常称为**穿脱法则**.

一般地, 对于 $a \in A$, 若存在 $b \in A$ 使得 $ab = e$, 则称 b 为 a 的一个**右逆**. 若存在 $c \in A$ 使得 $ca = e$, 则称 c 为 a 的一个**左逆**. 类似于命题 1.1.2 的证明可得若 A 上的运算满足结合律, 且 $a \in A$ 有右逆 b 和左逆 c, 则 $b = c$, 从而 a 可逆且 $a^{-1} = b = c$.

从符号上来说, 若 A 上的运算写为加法 "$+$", 则 A 中元素 a 和 b 的运算结果记为 $a + b$, 并称其为 a 与 b 的**和**. 若运算 "$+$" 满足结合律, 这时元素的幂就成为倍数, 即对于 $a \in A$, n 为正整数, 定义

$$na = \underbrace{a + a + \cdots + a}_{n\text{个}}.$$

类似地, 对任意正整数 m, n 有

$$ma + na = (m + n)a$$

和

$$n(ma) = (mn)a.$$

设 A 上的运算记为加法 "$+$", 若 A 中有单位元, 则该元素记为 0 并称为**零元**, 即对任意 $a \in A$ 有

$$0 + a = a + 0 = a.$$

这时也定义 $0a = 0$, 即元素的 0 倍为零元. 这里要注意等式左、右两端符号 0 的含义是不同的, 左端的 0 表示的是整数 0, 而右端的 0 是 A 中的零元. 若 $a \in A$ 可逆, 则 a 的唯一逆元记为 $-a$, 并称其为 a 的**负元**.

《代数学 (一)》第一章中定义了等价关系, 所谓等价关系就是一个满足自反性、对称性和传递性的二元关系. 设 R 是集合 A 上的一个等价关系, 对于 $a \in A$, 所有与 a 等价的元素做成的集合 $\overline{a}$ 为 R 的一个等价类, a 称为该等价类的一个代表元. 注意到等价类代表元是不唯一的, 等价类 $\overline{a}$ 中的任一元素都是 $\overline{a}$ 的代表元. A 在等价关系 R 下的所有等价类构成的集合称为 A 关于 R 的**商集**, 记为 A/R. 若 A 上有运算 "$\cdot$", 在商集 A/R 上定义

$$\overline{a} \circ \overline{b} = \overline{a \cdot b},$$

则 "$\circ$" 是否是 A/R 上的运算?

由于商集中的元素是等价类, 等价类的代表元选取不一定唯一, 而 “$\circ$” 是由等价类的代表元来定义的. 所以若 “$\circ$” 是 A/R 上的运算, 由运算结果的唯一性, 必然满足如下条件:

$$\text{若 } \overline{a_1}=\overline{a_2} \text{ 且 } \overline{b_1}=\overline{b_2}, \text{则 } \overline{a_1\cdot b_1}=\overline{a_2\cdot b_2}. \tag{1.1}$$

容易验证这个必要条件也是充分的, 即若条件 (1.1) 成立, 则 “$\circ$” 是 A/R 上的运算. 条件 (1.1) 称为等价类的运算与代表元的选取无关, 这时称集合 A 上满足条件 (1.1) 的运算 “$\cdot$” 与 A 上的等价关系 R **相容**, 也称 “$\circ$” 是由 A 上的运算 “$\cdot$” **诱导出**的商集 A/R 上的运算. 进一步地, 容易验证若 A 上的运算 “$\cdot$” 满足交换律或 (和) 结合律, 则它诱导出的商集 A/R 上的运算 “$\circ$” 也满足交换律或 (和) 结合律. 若 A 有单位元 e, 则易知 $\bar{e}$ 为 A/R 的单位元; 若 $a\in A$ 有逆元 a^{-1}, 则 $\overline{a^{-1}}$ 为 $\bar{a}\in A/R$ 的逆元.

习题 1.1

1. 判断下列论断是否正确, 若正确, 给出简要证明, 否则举反例说明:

(1) 设 $\mathbb{R}^+$ 是所有正实数构成的集合,

$$\begin{aligned}\mathbb{R}&\to\mathbb{R}^+\\ y&\mapsto y^2\end{aligned}$$

是一个映射;

(2) 在 $\mathbb{R}$ 中, 对任意 $x,y\in\mathbb{R}$, 定义

$$xRy\Leftrightarrow|x-y|\leqslant 3,$$

关系 R 是一个等价关系;

(3) 在 $\mathbb{Z}$ 中, 对任意 $m,n\in\mathbb{Z}$, 定义

$$mRn\Leftrightarrow 2\nmid m-n,$$

关系 R 不是一个等价关系;

(4) 在 n 阶复矩阵集合 $\mathbb{C}^{n\times n}$ 中, 对任意 $M,N\in\mathbb{C}^{n\times n}$, 定义

$$MRN\Leftrightarrow \text{存在 } P,Q\in\mathbb{C}^{n\times n}, \text{使得 } M=PNQ,$$

关系 R 是一个等价关系;

(5) 一个非空集合上的关系可以同时是等价关系和偏序关系.

2. 设 A, B 是两个集合, $f:A\to B$ 和 $g:B\to A$ 是映射. 如果 gf 为集合 A 上的恒等变换 id_A, 那么称 g 为 f 的一个左逆映射. 如果 fg 为集合 B 上的恒等变换 id_B, 那么称 g 为 f 的一个右逆映射. 如果 g 既是 f 的左逆映射又是 f 的右逆映射, 那么称 g 为 f 的逆映射. 证明

(1) f 有左逆映射当且仅当 f 是单射, f 有右逆映射当且仅当 f 是满射, 从而 f 有逆映射当且仅当 f 是双射;

(2) 若 f 有左逆映射 g, 同时又有右逆映射 h, 则 $g = h$.

3. 设 A, B 是两个有限集合, $|A| = m$, $|B| = n$, 证明

(1) 映射 $f : A \to B$ 的个数为 n^m;

(2) 若 $f : A \to B$ 为单射, 则有 $m \leqslant n$; 进一步地, 若 $m \leqslant n$, 则从 A 到 B 的单射个数为

$$n(n-1)\cdots(n-m+1) = \frac{n!}{(n-m)!};$$

(3) 若 $f : A \to B$ 为满射, 则 $m \geqslant n$; 进一步地, 若 $m \geqslant n$, 则从 A 到 B 的满射个数为

$$\sum_{j=0}^{n}(-1)^{n-j}\binom{n}{j}j^m;$$

(4) 设 $m = n$, 则从 A 到 B 的单射也是满射, 从 A 到 B 的满射也是单射, 从而从 A 到 B 的单射或满射都是双射.

4. 在 $\mathbb{Z}$ 中, 考虑如下定义的两个等价关系 $\sim_1$ 和 $\sim_2$. 对任意 $m, n \in \mathbb{Z}$, 定义

$$m \sim_1 n \Leftrightarrow 6 \mid m-n, \quad m \sim_2 n \Leftrightarrow 2 \mid m-n.$$

(1) 描述 $\sim_1$ 诱导的 $\mathbb{Z}$ 的划分 $\mathbb{Z}_6$ 和 $\sim_2$ 诱导的 $\mathbb{Z}$ 的划分 $\mathbb{Z}_2$;

(2) 以上两个划分中, 是否存在一个比另一个更细? 为什么?

5. 判断以下给出的集合上的运算是否满足结合律或者交换律. 若答案为否, 请举例说明原因:

集合	运算	结合律	交换律
$\mathbb{Z}$	$a * b = a - b$		
$\mathbb{Z}^+$	$a * b = 2^{ab}$		
$\mathbb{C}^{2\times 2}$	$M * N = MN - NM$		

6. 设 $A = \mathbb{Q} \setminus \{-1\}$, 即不等于 -1 的所有有理数构成的集合, 对于 $a, b \in A$, 定义 $\circ$ 为

$$a \circ b = a + b + ab.$$

证明 $\circ$ 是集合 A 上的运算, 且满足交换律和结合律. 进一步判断 A 中是否有单位元? A 中元素是否有逆元? 在有逆元时求出元素 $a \in A$ 的逆元.

7. 考虑 $\mathbb{Q}$ 上的等价关系:

$$u \sim v \Leftrightarrow u - v \in \mathbb{Z},$$

证明 $\mathbb{Q}$ 上的加法与等价关系 $\sim$ 相容.

1.2　半群与群

下面我们将给出代数结构群、环、域的概念, 一些例子并讨论它们的基本性质.

定义 1.2.1　设 S 为一非空集合, 其上有一个代数运算, 且运算满足结合律, 则称 S 为一个**半群**. 进一步地, 若半群 S 有单位元, 则称 S 为**幺半群**.

例 1.2.1　自然数集 $\mathbb{N}$ 在通常数的加法运算下做成一个幺半群, 它的零元为自然数 0. $\mathbb{N}$ 在通常数的乘法运算下也做成一个幺半群, 它的单位元为自然数 1. 正整数集 $\mathbb{Z}^+$ 在通常数的加法运算下做成一个半群, 它没有零元. 而 $\mathbb{Z}^+$ 在通常数的乘法运算下做成一个幺半群, 它的单位元为正整数 1.

注意到半群中的运算满足结合律, 所以半群中有幂 (或倍式). 同样幺半群中可逆元的逆元唯一, 也有穿脱法则等.

例 1.2.2　整数集 $\mathbb{Z}$ 在通常数的加法运算下做成一个幺半群, 它的零元为整数 0; 并且每个元素都有负元, 即它的相反数. 而 $\mathbb{Z}$ 在通常数的乘法运算下也做成一个幺半群, 它的单位元为整数 1; 并且除 ± 1 外, 其他元素都没有逆元.

例 1.2.3　设 $F^{n\times n}$ 为域 F 上所有 n 阶方阵构成的集合, 运算为通常矩阵的乘法, 则 $F^{n\times n}$ 做成一个幺半群, 它的单位元为单位矩阵 I, 可逆元为所有可逆矩阵.

定义 1.2.2　设 G 是一个非空集合, 其上有一个代数运算, G 在这个运算下做成一个幺半群 (即运算有结合律, 且 G 中有单位元), 并且 G 中每个元素都有逆元, 则称 G 为一个**群**.

群一定是幺半群, 但反之不成立. 例如自然数集 $\mathbb{N}$ 在通常数的加法运算下做成一个幺半群, 但它不是群.

若群 G 的运算满足交换律, 则称 G 为**交换群**, 或称为 **Abel (阿贝尔) 群**. 元素个数有限的群称为**有限群**, 元素个数无限的群称为**无限群**, 有限群中的元素个数称为该群的**阶**, 通常有限群 G 的阶记为 $|G|$.

例 1.2.4　若运算为通常数的加法, 则 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是交换群, 零元都是数 0, 数 a 的负元是 a 的相反数. 若运算为通常数的乘法, 则 $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}, \mathbb{R}^* = \mathbb{R}\setminus\{0\}, \mathbb{C}^* = \mathbb{C}\setminus\{0\}$ 也都是交换群, 单位元都是数 1, 非零数 a 的逆元为 a 的倒数. 但是 $\mathbb{Z}^* = \mathbb{Z}\setminus\{0\}$ 在通常数的乘法下不构成群, 因为除 ± 1 外, $\mathbb{Z}^*$ 中其余元素都没有逆元.

例 1.2.5　令 μ_n 为 n 次单位复根的集合, 即

$$\mu_n = \{a \in \mathbb{C} \mid a^n = 1\},$$

运算为通常的复数乘法. 首先需要确认复数乘法确实是 μ_n 中的运算, 事实上, 若 $a, b \in \mu_n$, 即 $a^n = 1, b^n = 1$, 则

$$(ab)^n = a^n b^n = 1,$$

故 $ab \in \mu_n$, 即运算结果在 μ_n 中, 而运算结果唯一是显然的. 运算的结合律在复数集合上成立, 自然在 μ_n 上成立. μ_n 中存在单位元, 即数 1. 并且任意 $a \in \mu_n$ 在 μ_n 中有逆 a^{-1}. 所以 μ_n 是一个群, 称为 n 次**单位根群**. 由于 $x^n = 1$ 有 n 个复根, 故 μ_n 的阶为 n. 进一步地,

$$\mu_n = \{\varepsilon_0, \varepsilon_1, \cdots, \varepsilon_{n-1}\},$$

其中 $\varepsilon_k = \mathrm{e}^{\mathrm{i}\frac{2k\pi}{n}} (= \varepsilon_1^k)$, $0 \leqslant k \leqslant n-1$. 特别地, $\mu_2 = \{1, -1\}$.

例 1.2.6 设 $\mathrm{GL}_n(F)$ 为域 F 上所有 n 阶可逆矩阵构成的集合, 运算为矩阵乘法, 则容易验证 $\mathrm{GL}_n(F)$ 是一个群, 称为域 F 上的 n 级**一般线性群**. 设 $\mathrm{SL}_n(F)$ 为数域 F 上所有行列式为 1 的 n 阶矩阵构成的集合, 运算仍为矩阵乘法, 则 $\mathrm{SL}_n(F)$ 也是一个群, 称为域 F 上的 n 级**特殊线性群**. 注意, 这两个群在 $n \geqslant 2$ 时都是非交换的.

命题 1.2.1 *设 S 为幺半群, 用 $U(S)$ 表示 S 中所有可逆元构成的集合, 则 $U(S)$ 在 S 的运算下构成一个群.*

证明 显然 S 的单位元 $e \in U(S)$, 故 $U(S)$ 非空. 由命题 1.1.3 知可逆元的乘积仍然是可逆元, 所以 S 的运算限制在 $U(S)$ 上是 $U(S)$ 上的运算. 运算的结合律显然, $U(S)$ 中有单位元 e, 仍由命题 1.1.3 知 $U(S)$ 中任一元素在 S 中的逆元 $a^{-1} \in U(S)$, 所以它也是 a 在 $U(S)$ 中的逆元. 故 $U(S)$ 为群. □

半群 S 中的可逆元也称为 S 的**单位**, 故称 $U(S)$ 为**幺半群 S 的单位群**.

例 1.2.7 设 M 为一个集合, T_M 表示 M 上的全体变换 (即 M 到自身的映射) 构成的集合, 定义 T_M 上的运算为映射乘法 (合成), 则 T_M 为一个幺半群, 单位元为恒等变换 id_M. 此幺半群的单位群记为 S_M, 称为集合 M 的**全变换群**. 由习题 1.1 第 2 题知幺半群 T_M 中的元素可逆当且仅当它是 M 到自身的双射. 所以 S_M 是 M 的全体可逆变换 (即 M 到自身的双射) 构成的集合, 运算仍为映射乘法 (合成).

特别地, 若集合 M 有限, 不妨设 $M = \{1, 2, \cdots, n\} =: [n]$. 显然 $\sigma \in S_M$ 当且仅当 $\sigma(1), \sigma(2), \cdots, \sigma(n)$ 是 $1, 2, \cdots, n$ 的一个排列. $[n]$ 到自身的双射也称为 $[n]$ 上的一个**置换**, 或为一个 n 元置换. 所有 n 元置换在置换乘法下构成的群 $S_{[n]}$ 称为 n **元对称群**, 也简记为 S_n. S_n 为有限群, 其阶为 n 元排列的个数, 即 $n!$.

下面给出群中一个基本的运算性质——消去律.

命题 1.2.2 *设 G 为群, 则 G 中有消去律, 即对任意 $a, b, c \in G$, 若 $ab = ac$, 或者 $ba = ca$, 则有 $b = c$.*

证明 若 $ab = ac$, 则等式两端同时左乘 a^{-1} 有

$$a^{-1}(ab) = a^{-1}(ac),$$

由结合律得 $(a^{-1}a)b = (a^{-1}a)c$, 即 $eb = ec$, 故 $b = c$.

若 $ba = ca$, 则等式两端同时右乘 a^{-1} 可推出 $b = c$. □

一般地, 若在半群中可由 $ab = ac$ 得到 $b = c$, 即可以消去左端的元素 a, 这称为**左消去律**. 而可由 $ba = ca$ 得到 $b = c$ 就称为**右消去律**. 例如在例 1.2.7 的半群 T_M 中, 在等式 $fg = fh$ 两端可左消去 f 当且仅当 f 为单射, 而在等式 $gf = hf$ 两端可右消去 f 当且仅当 f 为满射. 所以在半群 T_M 中既没有左消去律, 也没有右消去律.

群是半群, 所以群中也有穿脱法则, 即对群 G 中元素 $a_1, a_2, \cdots, a_m$ 有

$$(a_1 a_2 \cdots a_m)^{-1} = a_m^{-1} \cdots a_2^{-1} a_1^{-1}.$$

但是在群 G 中, 乘积的幂不一定等于幂的乘积, 即存在 $a, b \in G$, $n \geqslant 2$ 为正整数, 但不一定有 $(ab)^n = a^n b^n$, 这是因为

$$(ab)^n = \underbrace{(ab)(ab)\cdots(ab)}_{n\text{ 个}},$$

而

$$a^n b^n = (\underbrace{aa\cdots a}_{n\text{ 个}})(\underbrace{bb\cdots b}_{n\text{ 个}}).$$

当然若对于 $a, b \in G$, a, b 可交换, 即 $ab = ba$, 则容易验证有 $(ab)^n = a^n b^n$.

注意到群中的元素都有逆元, 所以对于群 G 中的元素 a, n 为正整数, 定义

$$a^{-n} = (a^{-1})^n,$$

即可以定义群中元素的负整数次幂 (或者负整数倍, 若群的运算写成加法). 这时幂运算法则依然成立, 即对任意 $a \in G$, m, $n \in \mathbb{Z}$, 有

$$a^m a^n = a^{m+n}$$

和

$$(a^m)^n = a^{mn}.$$

习题 1.2

1. 设 S 为幺半群, $a, b \in S$, 若 ab 可逆, 是否有 a 和 b 均可逆? 证明或举出反例.

2. 设 S 为幺半群, $a_1, a_2, \cdots, a_m \in S$ 且两两可交换, 证明 $a_1 a_2 \cdots a_m$ 可逆当且仅当 a_1, a_2, $\cdots$, a_m 均可逆.

3. 设 A 是一个非空集合, 其上有一个运算, e_l (或 e_r) $\in A$. 若对任意 $a \in A$, 均有 $e_l a = a$ (或 $ae_r = a$), 则称 e_l (或 e_r) 为 A 的一个左 (或右) 单位元. 对于 $a \in A$, 若存在 $b \in A$ 使得 $ba = e_l$ (或 $ab = e_r$), 则称 b 为 a 的一个左 (或右) 逆元.

(1) 若 A 中运算满足结合律, 存在左单位元, 且 A 中每个元素都有左逆元, 证明 A 是一个群;

(2) 若 A 中运算满足结合律, 存在右单位元, 且 A 中每个元素都有右逆元, 证明 A 是一个群.

4. 设 G 为具有一个运算的非空集合, 已知该运算满足结合律, 并且对于 G 中任意两个元素 a, b, 方程 $ax=b$ 和 $xa=b$ 都在 G 中有解, 证明 G 是一个群.

5. 设 G 是一个群, $a,b\in G$, 如果 $aba^{-1}=b^r$, 其中 r 是一个整数, 证明对任意正整数 i, 有 $a^iba^{-i}=b^{r^i}$.

6. 设 G 是一个群, 如果对于任意 $a,b\in G$ 都有 $(ab)^2=a^2b^2$, 证明 G 为交换群.

7. 设 $n\geqslant 3$, 在 n 元对称群 S_n 中找两个元素 σ, τ 使得 $\sigma\tau\neq\tau\sigma$. 由此可知 S_n 不是交换群.

1.3 环与域

定义 1.3.1 设 R 是一非空集合, R 上有两种代数运算, 分别称为加法和乘法, 记为 "$+$" 和 "$\cdot$", 且满足

(1) R 对加法做成交换群, 即 $(R,+)$ 为交换群.

(2) R 对乘法做成幺半群, 即 $(R,\cdot)$ 为幺半群.

(3) 乘法对加法的左、右分配律成立, 即对任意 $a,b,c\in R$, 有

$$a(b+c)=ab+ac,\quad (b+c)a=ba+ca.$$

则称 R 为一个**环**.

注意环中乘法不一定满足交换律, 满足乘法交换律的环称为**交换环**. 另外为讨论方便起见, 特别是一些有重要意义的环中都有乘法单位元, 所以定义中特别要求环中有乘法单位元, 但《代数学 (一)》中定义的环不要求这一点. 环中的乘法单位元称为**环的单位元**, 常记为 1, 而环中加法的零元也称为**环的零元**, 记为 0. 在环 R 中, $(R,+)$ 为交换群, 所以环中的加法满足消去律. 对乘法来说, R 的可逆元也称为环 R 的**单位**. 由于 $(R,\cdot)$ 为幺半群, 故有单位群, 幺半群 $(R,\cdot)$ 的单位群称为**环 R 的单位群**, 记为 $U(R)$. 环中的加法和乘法都满足结合律, 所以环中元素既有倍数 (包括负整数倍), 也有幂.

例 1.3.1 由《代数学 (一)》第三章知域 F 上的所有一元多项式集合 $F[x]$ 在多项式加法和乘法下构成一个交换环, 其中零元即零多项式 0, 单位元为零次多项式 1, 而它的单位群 $U(F[x])$ 为 F^*, 即域 F 的所有非零元构成的乘法群. 称 $F[x]$ 为域 F 上的**一元多项式环**.

例 1.3.2 设 $R=\{0\}$, 定义 $0+0=0$, $0\cdot 0=0$, 在这两种运算下 R 构成一个环, 称这个环为**零环**, 它的零元和单位元都是 0. 显然它是交换环.

例 1.3.3　整数集 $\mathbb{Z}$ 在通常的整数加法和乘法运算下构成一个交换环, 称为**整数环**. 设 $k>1$ 为正整数, 则所有 k 的倍数构成的集合 $k\mathbb{Z}=\{kn \mid n\in\mathbb{Z}\}$ 在通常的整数加法和乘法运算下不构成环, 因为 $k\mathbb{Z}$ 中没有单位元. 虽然它满足环中除乘法单位元这个要求外的所有条件.

例 1.3.4　设 $R=F^{n\times n}$, 即域 F 上所有 n 阶方阵构成的集合, 运算为通常的矩阵加法和矩阵乘法, 则 R 构成一个环, 称为域 F 上的**全矩阵环**. 此环在 $n\geqslant 2$ 时为非交换环, 单位元是单位矩阵, 单位群为 $\mathrm{GL}_n(F)$.

命题 1.3.1　*设 R 是环, 则对任意 $a\in R$, 有 $0a=a0=0$.*

证明　由于 $(0+0)a=0a$, 由分配律得

$$0a+0a=0a=0a+0,$$

再由加法的消去律得 $0a=0$. 同理可证 $a0=0$. □

若环 R 中单位元 $1=0$, 则对于任意 $a\in R$, 由命题 1.3.1 有

$$a=a\cdot 1=a\cdot 0=0,$$

即 $R=\{0\}$ 为零环. 所以若 $R\neq\{0\}$, 则一定有 $1\neq 0$, 从而 $|R|\geqslant 2$ 且环 R 中的零元 0 是不可逆的. 环中有单位元, 但也并不是环中每个非零元都有逆, 环中乘法可逆的元素称为**可逆元** (或**单位**). 环 R 中所有可逆元在乘法下构成一个群, 即环 R 的单位群 $U(R)$.

定义 1.3.2　*若环 R 至少含有 2 个元素且其中每个非零元都可逆, 则称 R 为***除环*** (*或***体***).*

由定义, 除环 R 的单位群 $U(R)$ 为 $R^*=R\backslash\{0\}$, 即 R 的所有非零元构成的乘法群.

不是所有环的乘法都满足消去律, 即对于 $a,b,c\in R$, $a\neq 0$, $ab=ac$ (或 $ba=ca$), 则不一定有 $b=c$ (群中乘法满足消去律是因为群中每个元素都可逆, 但环中并不是每个非零元都可逆). 自然若 a 有逆, 且 $ab=ac$ (或 $ba=ca$), 则同样可得 $b=c$. 所以, 除环中的乘法满足消去律. 设 H 为除环, $a,b\in H$ 且 $a\neq 0$, 则方程 $ax=b$ 和 $xa=b$ 在 H 中有解, 分别为 $a^{-1}b$ 和 ba^{-1} (形式上说, 除环中可以做除法).

定义 1.3.3　*设 R 为环, $a\neq 0$, 若存在 $b\neq 0$ 使得 $ab=0$, 则称 a 是 R 的一个***左零因子***. 若存在 $c\neq 0$ 使得 $ca=0$, 则称 a 是 R 的一个***右零因子***. 左零因子或右零因子都称为 R 的***零因子***.*

设 a 为环 R 的一个左零因子, 即存在 $b\neq 0$ 使得 $ab=0$. 若 a 为可逆元, 则有

$$b=a^{-1}(ab)=0,$$

矛盾. 这表明环中的左零因子一定不可逆. 同理, 环中的右零因子也不可逆. 故除环中没有左零因子, 也没有右零因子. 显然交换环的左零因子也是右零因子, 反之亦然. 容易证明在域 F 上的全矩阵环 $F^{n\times n}$ 中, 元素 A 为左零因子当且仅当 A 不可逆也当且仅当 A 为右零因子, 所以 $F^{n\times n}$ 中的左零因子也是右零因子, 虽然 $F^{n\times n}$ 不是交换环.

例 1.3.5 设 R 为环, X 为一非空集合. 从 X 到 R 的所有映射的集合 R^X 在逐点加法和逐点乘法下构成一个环. 所谓映射的逐点加法和逐点乘法定义为对任意映射 $f, g \in R^X$ 和任意 $x \in X$,

$$(f+g)(x) = f(x) + g(x)$$

和

$$(fg)(x) = f(x)g(x).$$

容易验证 R^X 交换当且仅当 R 交换, 若 R 不是零环且 $|x| \geqslant 2$, 则 R^X 有零因子.

定义 1.3.4 至少含有 2 个元素且没有零因子的交换环称为**整环**.

容易验证整数环 $\mathbb{Z}$ 和域 F 上的一元多项式环 $F[x]$ 都是整环.

定义 1.3.5 交换除环称为**域**.

由定义知域 F 是一个集合, 至少含有 2 个元素, 在 F 中有两个代数运算, 加法 "$+$" 和乘法 "$\cdot$", 且满足 $(F,+)$ 为交换群, $(F^*,\cdot)$ 为交换群, 它就是域 F 的单位群, 也称为域 F 的乘法群, 其中 $F^* = F \setminus \{0\}$, 且乘法对加法的分配律成立. 元素个数有限的域称为**有限域**. 显然 $\mathbb{Q}$, $\mathbb{R}$ 和 $\mathbb{C}$ 在通常数的加法和乘法下构成域, 分别称为**有理数域**、**实数域**和**复数域**, 它们都是无限域. 但是整数集 $\mathbb{Z}$ 在通常数的加法和乘法下不是域, 而是一个整环.

域是整环, 但整环不一定是域. 例如 $\mathbb{Z}$ 和 $F[x]$ 都是整环, 但它们不是域. 然而容易证明有限整环一定是域.

例 1.3.6 设 $\mathbb{F}_2 = \{0,1\}$, 定义

$$\begin{aligned} &0+0 = 1+1 = 0,\\ &0+1 = 1+0 = 1,\\ &0\cdot 0 = 0\cdot 1 = 1\cdot 0 = 0,\\ &1\cdot 1 = 1, \end{aligned}$$

则在这两个运算下, $\mathbb{F}_2$ 构成一个域, 这是一个有限域.

习题 1.3

1. 设 R 为交换环, 对于任意 $a, b \in R$, 定义

$$a \oplus b = a + b - 1, \quad a \odot b = a + b - ab,$$

证明 R 在运算 $\oplus$, $\odot$ 下也构成一个交换环.

2. 设 R 为环, 定义 $a - b = a + (-b)$, 证明: 对任意 $a, b, c \in R$, 有

$$-(a+b)=(-a)+(-b)=-a-b,$$
$$-(a-b)=(-a)+b,$$
$$-(ab)=(-a)b=a(-b),$$
$$(-a)(-b)=ab,$$
$$a(b-c)=ab-ac.$$

3. 设 R 为环, $a,b\in R$, 且 a, b 可交换, 证明二项式定理: 对任意正整数 n,

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

4. 给出一个没有乘法消去律的环的例子.

5. 证明整环中有消去律.

6. 设 R 为环, $a\in R$, $a\neq 0$, 且存在 $b\in R$, $b\neq 0$ 使得 $aba=0$, 证明 a 是 R 的一个左零因子或右零因子.

7. 设 R 为有限环, a, $b\in R$ 且 $ab=1$, 证明 $ba=1$.

8. 设 R 为环, a, $b\in R$ 且 $ab=1$ 但是 $ba\neq 1$, 证明有无穷多个 $x\in R$ 满足 $ax=1$.

9. 设 R 为环, $a\in R$. 如果存在正整数 n 使得 $a^n=0$, 就称 a 为**幂零元**. 证明若 a 为幂零元, 则 $1-a$ 可逆.

10. 设 R 为环, $a,b\in R$. 设 $1-ab$ 可逆, 证明 $1-ba$ 也可逆并求出 $(1-ba)^{-1}$.

11. 证明有限整环是域.

12. 设 R 为除环, a, $b\in R$ 且 $ab\neq 0$, 1, 证明华罗庚等式

$$a-(a^{-1}+(b^{-1}-a)^{-1})^{-1}=aba.$$

13. 设 R 为一个无零因子环, $e\in R$ 满足对所有 $a\in R$ 有 $ea=a$, 证明 e 为 R 的单位元.

14. 设 D 是一个整环, 在 D 中解方程 $x^2=1$.

15. 设 R 为环, 若 $u\in R$ 存在右逆元但不唯一, 证明 u 有无穷多个右逆元.

1.4　整数模 n 的剩余类环

设 n 为正整数, 在整数集 $\mathbb{Z}$ 上定义关系 $\sim$ 如下: 对任意 a, $b\in\mathbb{Z}$,

$$a\sim b \text{ 当且仅当 } n\mid(a-b), \text{ 或记为 } a\equiv b\ (\mathrm{mod}\ n).$$

容易验证 $\sim$ 是整数集 $\mathbb{Z}$ 上的一个等价关系. 在该等价关系下, $j\in\mathbb{Z}$ 的等价类为

$$\overline{j}=\{kn+j\mid k\in\mathbb{Z}\},$$

且该等价关系的商集为

$$\mathbb{Z}_n := \mathbb{Z}/\sim = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

若对 $a_1, b_1, a_2, b_2 \in \mathbb{Z}$ 有 $\overline{a_1} = \overline{a_2}$ 和 $\overline{b_1} = \overline{b_2}$, 即 $n \mid (a_1 - a_2)$ 且 $n \mid (b_1 - b_2)$, 则由

$$(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$$

和

$$a_1 b_1 - a_2 b_2 = (a_1 - a_2)b_1 + a_2(b_1 - b_2),$$

得到

$$n \mid ((a_1 + b_1) - (a_2 + b_2))$$

和

$$n \mid (a_1 b_1 - a_2 b_2),$$

即 $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ 且 $\overline{a_1 b_1} = \overline{a_2 b_2}$. 故整数环 $\mathbb{Z}$ 上的加法和乘法运算诱导了商集 $\mathbb{Z}_n$ 上的运算, 仍称其为加法和乘法并分别记为 $+$ 和 $\cdot$, 即对任意 $\overline{a}, \overline{b} \in \mathbb{Z}_n$, 有

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} \cdot \overline{b} = \overline{ab}.$$

又 $\mathbb{Z}_n$ 上的加法和乘法运算具有 $\mathbb{Z}$ 上的加法和乘法运算所满足的交换律、结合律和分配律, 所以 $\mathbb{Z}_n$ 在这样的加法和乘法运算下构成一个交换环, 称其为**整数模 n 的剩余类环**. 环 $\mathbb{Z}_n$ 中有 n 个元素, 所以它是有限环. $\mathbb{Z}_n$ 的单位群也称为**整数模 n 的乘法群**, 记作 $U(n)$, 这是一个有限交换群.

显然, 若 $n = 1$, 则 $\mathbb{Z}_1 = \{\overline{0}\}$, 即 $\mathbb{Z}_1$ 为零环, 它的单位群 $U(1) = \{\overline{0}\}$ 是 1 阶群.

例 1.4.1 若 n 是合数, 不妨设 $n = ab$, 其中 $1 < a, b < n$, 则在 $\mathbb{Z}_n$ 中, $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$, 但是

$$\overline{a}\,\overline{b} = \overline{ab} = \overline{n} = \overline{0},$$

故 $\overline{a}$ 和 $\overline{b}$ 都是 $\mathbb{Z}_n$ 的零因子, 所以 $\mathbb{Z}_n$ 不是整环.

命题 1.4.1 *设 $n \geqslant 2$, $k \in \mathbb{Z}$, 则 $\overline{k}$ 在 $\mathbb{Z}_n$ 中可逆当且仅当 k 与 n 互素.*

证明 由定义, $\overline{k}$ 在 $\mathbb{Z}_n$ 中可逆当且仅当存在 $\overline{l} \in \mathbb{Z}_n$ 使得 $\overline{k} \cdot \overline{l} = \overline{1}$, 即 $n \mid (1 - kl)$. 从而存在 $t \in \mathbb{Z}$ 使得

$$kl + tn = 1,$$

这就等价于 k 与 n 互素. □

命题 1.4.1 告诉我们整数模 n 的乘法群 $U(n)$ 为有限群, 其阶为 $\phi(n)$, 这里 $\phi(n)$ 为 Euler(欧拉) ϕ-函数, 即小于 n 且与 n 互素的自然数的个数.

推论 1.4.1 *环 $\mathbb{Z}_n$ 为域当且仅当 n 为素数.*

证明　若 n 为素数, 则对任意 $1 \leqslant k \leqslant n-1$, k 与 n 互素, 所以 $\overline{k} \in \mathbb{Z}_n$ 可逆, 即 $\mathbb{Z}_n$ 中每个非零元都可逆, 所以 $\mathbb{Z}_n$ 为域.

反之, 若 n 不是素数, 则例 1.4.1 告诉我们 $\mathbb{Z}_n$ 有零因子, 即 $\mathbb{Z}_n$ 中有非零不可逆元, 所以 $\mathbb{Z}_n$ 不是域. □

由推论 1.4.1 知, 对于任意素数 p, 存在 p 元域 $\mathbb{Z}_p$, 这是一个有限域. 例 1.3.6 就是 $p=2$ 时的域 $\mathbb{Z}_2$.

习题 1.4

1. 证明在 p 元域 $\mathbb{Z}_p$ 中有

$$(a+b)^{p^k} = a^{p^k} + b^{p^k},$$

其中 $a, b \in \mathbb{Z}_p$, k 为任意正整数.

2. 给出一个有限非交换群 G, 使得对任意 $a \in G$ 均有 $a^4 = e$.

3. 求出方程 $x^2 - 1 = 0$ 在环 $\mathbb{Z}_{360}$ 中的全部解.

4. 证明群 $U(3^5)$ 中一定有一个元素 g 使得 $U(3^5)$ 中每个元素都是 g 的幂. 这个结论对群 $U(2^5)$ 是否正确?

5. 在 $\mathbb{Z}_{29}$ 中计算 $\overline{28^{60}}$.